STATEMENT OF WORK
b(3) Engineering Services

1.0 INTRODUCTION

1.1 BACKGROUND

Naval Information Warfare Center Pacific's (NIWC) Space and Intelligence Systems (SIS) Division works to enhance the Navy's and partner nations' Maritime Domain Awareness (MDA) capability.

Illegal, unreported, and unregulated (IUU) fishing activities is a global problem that threatens economic security and natural resources for US and partner nations.

GFW has developed algorithms to detect transshipments between vessels that may or may not be engaged in IUU. The USN's b(3) is a web-based maritime situational awareness tool with a requirement to provide detections of near-real time transshipments. Currently, GFW algorithms are available on the Application Programming Interface (API) but not available in near-real time. Near-real-time delivery will require additional engineering and possibly a push to the b(3) API instead of b(3 pulling the data from GFW API. In addition, GFW focuses on IUU, therefore the accuracy of non IUU transshipments requires validation prior to ingestion into b(3)

b(3) can ingest, correlate, and display track and other situational awareness data from non-profit organizations, as well as MDA partner nation data and display to users based on user and community access rules established in the b(3) platform.

1.2 SCOPE

The purpose of this effort is to improve partner nation MDA through data sharing. Access to key data sources through b(3) will allow for collaboration within the country and between the country and MDA partner nations.

Contractor engineers will provide technical assistance to the NIWC b(3) team to validate encounters at sea and enable these transshipments in b(3 in near-real time. In addition, the contractor engineer will consult with b(engineers to build a transshipment service b(3) which will utilize b(3 data sources instead of relying on GFW data.

2.0 SERVICE REQUIREMENTS

The contractor shall:

2.0.1 Validate transshipment data of both IUU and non-IUU events.

2.0.2 Provide transshipment data either sent to the b(3) API or provided via GFW's API for ingestion into b(3) (CDRL A001).

2.0.3 Provide rendezvous algorithm to the Government. (CDRL A002).

2.0.4 Consult with b(engineers to build a transshipment service b(3) which will utilize b(3 data sources instead of relying on GFW data.(CDRL A003).

3.0 DELIVERABLES

The contractor shall deliver timely work products and services that conform to the requirements of this order. Final inspection and acceptance of services delivered is performed by the Technical POC.

CDRL	*Deliverable*	*Content*	*Due Date*	*Recipient*
A001	Transshipment data	Transshipment data for both IUU and non-IUU events	As required	Technical POC
A002	Rendezvous Algorithm		EOC	Technical POC
A003	b(3) Transshipment Service	b(3) transshipment service that uses b(3) data sources instead of relying on GFW data	EOC	Technical POC

4.0 TRAVEL

The contractor is not required to travel in support of this effort.

5.0 PLACE OF PERFORMANCE

The work will be done at the contractor's facility.

6.0 SECURITY

The work under this contract is UNCLASSIFIED. The contractor does not require a Common Access Card (CAC) or Defense Biometric Identification System (DBIDS) in the performance of the contract. All work will be done at the contractor's site.

Pursuant to DoDM 5200.01 and DoDI 5200.48, the contractor shall provide adequate security for all CUI and Unclassified DoD information passing through non-DoD information system including all subcontractor information systems utilized on contract. If the contractor originates, adds to, or changes any of the DoD information, it must be marked in accordance with DODI 5200.48 and handled properly. The contractor shall disseminate CUI and unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the contract, and privileged contract information (e.g., program schedules, contract-related tracking).

6.0.1 Operations Security (OPSEC): OPSEC is a five step analytical process (identify critical information; analyze the threat; analyze vulnerabilities; assess risk; develop countermeasures) that is used as a means to identify, control, and protect unclassified and unclassified sensitive information associated with U.S. national security related programs and activities. All personnel working under this task will at some time handle, produce or process Critical Information or Critical Program Information, and therefore all Contractor personnel must practice OPSEC. All work is to be performed in accordance with DoD OPSEC requirements.

6.0.2 Operations Security (OPSEC) Requirements: Security programs are oriented towards protection of classified information and material. Operations Security (OPSEC) is an operations function, which involves the protection of any critical information – focusing on unclassified information that may be susceptible to adversary exploitation. Pursuant to DoDD 5205.02E SECNAVINST 3070.2A, and NAVWARINST 3432.1, NAVWAR/NIWC Atlantic/NIWC Pacific's OPSEC program implements requirements in DoD 5205.02-M – OPSEC Program Manual. Note: OPSEC requirements are applicable when contract personnel have access to classified information, unclassified Critical Program Information (CPI), Controlled Unclassified Information (CUI) or Department of Navy (DoN) networks.

6.0.3 Local and Internal OPSEC Requirement: Contractor personnel, including subcontractors if applicable, shall adhere to the OPSEC program policies and practices as cited in the NAVWARINST 3432.1 and existing local site OPSEC procedures. The Contractor shall development their own internal OPSEC program specific to the contract and based on NAVWAR/NIWC Atlantic/NIWC Pacific OPSEC requirements. The Contractor's program shall identify the current contractor site OPSEC Officer/Coordinator/POC.

6.0.4 OPSEC Training: Contractor shall track and ensure applicable personnel receive initial and annual OPSEC awareness training. Training may be provided by the government or by the contractor's OPSEC Manager. Contractor training shall include, at a minimum, cover OPSEC as it relates to contract work; discuss the Critical Information applicable in the contract; applicable review of government Critical Information and Indicators List(s) (CIIL); social media awareness and vulnerabilities; local threats; how to protect, transmit, and destroy controlled unclassified information; risks and guidance pertaining to geolocation-capable devices, applications, and services; and OPSEC review procedures for public release. The Contractor shall ensure that training materials developed by the Contractor shall be reviewed by the NAVWAR/NIWC Atlantic/NIWC Pacific OPSEC Officer, who will ensure it is consistent with NAVWAR/NIWC Atlantic/NIWC Pacific OPSEC policies. OPSEC training requirements are applicable for personnel during their entire term supporting NAVWAR/NIWC Atlantic/NIWC Pacific contracts and for the duration of DoN Network access.

6.0.5 NAVWAR/NIWC Atlantic/NIWC Pacific OPSEC Program: If required, the Contractor shall participate in NAVWAR/NIWC Atlantic/NIWC Pacific OPSEC program briefings and working meetings, and complete any required OPSEC survey or data call within the timeframe specified.

7.0 GOVERNMENT FURNISHED PROPERTY (GFP)

None applicable.

8.0 POINT OF CONTACT:

NIWC Pacific Technical POC:
b(6) [redacted]